Electron Commer Res (2010) 10: 423–440
DOI 10.1007/s10660-010-9062-0

The impact of perceived privacy risks on organizations' willingness to share item-level event data across the supply chain

Markus Eurich · Nina Oertel · Roman Boutellier

Published online: 7 October 2010

Abstract When information is available about the path, on which individual items move through the real world, many beneficial applications can be designed. The necessary data can be generated through attaching identifiers to items and deploying suitable readers all over the supply chain that capture the information on the identifiers. Organizations only have access to data about item movements within their organizational boundaries. Therefore sharing of data between organizations is required to gain full visibility. However, the willingness of organizations to share data is considered to be low. In this paper we present the results of a study that aimed at investigating the actual willingness of companies to share item-level data and at exploring the perceived privacy risks that may restrain companies from sharing item-level data. From the findings, requirements for the design of inter-organizational data sharing infrastructures are derived.

Keywords Information sharing · Privacy risks · Event data · Internet of things

M. Eurich (✉)
SAP (Schweiz) AG, Research Center Zurich, Kreuzplatz 20, 8008 Zurich, Switzerland
e-mail: meurich@ethz.ch

N. Oertel
SAP AG, Research Center Karlsruhe, Vincenz-Priessnitz-Strasse 1, 76131 Karlsruhe, Germany

M. Eurich · R. Boutellier
D-MTEC, TIM, Swiss Federal Institute of Technology (ETH), Scheuchzerstrasse 7, 8092 Zurich, Switzerland

N. Oertel
Chair of BA and IS, University of Mannheim, L 15, 1-6, 68161 Mannheim, Germany

1 Introduction

The Internet is extending its reach to the real world through integration of technologies such as radio frequency identification (RFID), wireless sensor and actuator networks, and networked embedded devices. An electronic network between physical objects that connects the physical and the digital world is termed as the *Internet of Things* [1]. The unique identification of single objects via unique serial numbers, e.g. the electronic product code (EPC), sophisticated identification technologies, e.g. RFID or 2D barcodes, and a network infrastructure, e.g. the EPCglobal network, enable tracking and tracing of product movements through the supply chain in form of item-level event data [2]. Event data refers to any kind of time-stamped data that was captured during a product's flow through the supply chain. In contrast to the current information processing paradigm, which only addresses product types, *item-level* refers to a granularity level at which each product is labeled with a unique identifier that allows addressing of each item individually. The Internet of Things' concept comprises that information about items is stored locally at the organizations which have captured the information and, if required, is then distributed across the supply chain via a tracking infrastructure [3, 4].

Electronic commerce (e-commerce) includes the electronic trade of physical and intangible goods like information. It also comprises meta-services that enable other types of e-commerce like electronic support for collaboration between businesses [5]. There are different natures of e-commerce like business-to-consumer (B2C), business-to-business (B2B), or administration-to-business. The B2C dimension of e-commerce refers mainly to purchasing goods over (cf. online shopping) and consuming services directly on (cf. online banking) the Internet. This aspect of e-commerce gained the most public attention, while the B2B potential of e-commerce seems less appreciated by a broad publicity. The B2B aspect is characterized by the use of the Internet to facilitate business, e.g. to exchange financial data [5]. Data sharing and data security are prerequisites for any e-commerce service or meta-service especially from a B2B perspective and in supply chains, in which various entities need to cooperate with each other. The benefits and the importance of inter-organizationally shared event data at item-level become evident when considering the current situation, i.e. an insufficient or nonexistent tracking infrastructure: the coordination in the supply chain is error-prone and time-consuming, which might lead to a high level of inventory, high labor cost, and stock outs. The sharing of item-level event data offers many benefits, including precise tracking and tracing of products [3] which is important for the generation of electronic pedigrees [6], enables targeted recalls [3], or improved vendor managed inventory and continuous replenishment programs [2]. Further expected benefits include automated counterfeit detection, fewer out-of-stocks, identification of shrinkage, and theft detection [7]. Tracking based applications that rely on inter-organizational data sharing have also been devised for many different industries, e.g. aerospace, automotive, consumer goods, and the pharmaceutical industry [6, 8–10]. On the basis of shared item-level event data even new e-commerce business opportunities can arise, like anti-counterfeiting services or services to ensure supply chain integrity by complying with regulations imposed by external authorities (e.g. legal, tax, and transport).

Despite all the potential benefits, however, tracking based applications are not yet a reality in an inter-organizational context. This is partly due to the fact that the infrastructure needed to capture and distribute item-level data has not been fully developed yet. Additionally, it is reported that companies are reluctant to share item-level data with their business partners, competitors and organizations unknown to them [8, 11]. Particularly privacy risks, which go along with shared event data, are suited to restrain enterprises' willingness to share item-level event data across the supply chain. It is not well understood what the exact nature of these privacy risks is. However, understanding the risks perceived by companies is a prerequisite for designing measures that mitigate the risks and thus allow the realization of tracking based applications. Only if the privacy requirements of companies are addressed in an appropriate way, the vision of the Internet of Things can become reality.

The research presented in this paper thus has three major objectives: (1) to verify whether the willingness is indeed as low as suggested in literature, we aim at describing the current sharing behavior and general willingness to share in selected companies, (2) the description of risks perceived by companies and the impact of these risks on the willingness to share data, (3) the elicitation of requirements for designing risk mitigating measures. To achieve the first two objectives, an empirical study was conducted, in which interviews with 16 experts from various industries were performed to assess their current sharing behavior, their willingness to share, and the perceived negative consequences of data sharing.

The remainder of the paper is organized as follows: after reviewing related work, the methodology of the study is presented. Next, the study results with regard to the current sharing behavior of participating companies as well as their willingness to share data are described. Privacy risks that may impact an organizations' sharing behavior are described and their impact on the willingness to share data assessed. The implications for the design of inter-organizational tracking based applications are discussed before concluding and giving an outlook on future research.

2 Related work

A lot of authors already engaged in inter-organizational data sharing and several studies claimed data sharing as basis of efficient coordination and source of performance in supply chains [12–14]. In conventional stock-keeping, management information is prevalently shared only one stage up or down the supply chain [14–16]. In Vendor Managed Inventory and Continuous Replenishment Programs data is shared with multiple stages in the supply chains but is restricted to information about the level of stock or demand forecasts [14]. Lee and Whang state that IT advancements have a great impact on the development of supply chains [14]. In order to effectively manage product movements, diverse technologies like the Internet, Enterprise Resource Planning systems, or Advanced Planning systems are deployed [14, 17]. Literature on data sharing, however, is limited when it comes to sharing of fine-granular data. Although it is understood that the reluctance to share fine-granular data might hamper the adoption of tracking infrastructures and tracking based applications, only few possible explanations for the reluctance to share item-level event data exist. Privacy risks

were identified as a main factor affecting companies' willingness to share item-level data [11, 18, 19]. The willingness to share data is lower the more expected negative consequences of a potential risk are realized. In extreme cases potential risks might even prevent companies from sharing any data at all.

The project "Building Radio Frequency IDentification for the Global Environment" (BRIDGE) project aims at investigating the potential of applications based on item-level data [20]. A study conducted within this project has investigated which kind of information organizations would be willing to share in a tracking-enabled environment and under which conditions. The results indicate that organizations are reluctant to share location information. Most companies are only willing to share information on a contractual basis, i.e. with companies that are known to them and with which clear agreements are met on what type of information is shared and under which conditions. According to a study of the BRIDGE project organizations in the automotive industry seem reluctant to shared item-level data. They would only share data which is absolutely necessary for a track-and-trace application with close business partners. However, several participants of the BRIDGE study in the automotive industry could not yet estimate the extent to which item-level data would be shared. By contrast, data would be shared with business partners to enable product tracking applications in the consumer goods industry. Information that may be shared includes pallet identification numbers and dispatch advices. Organizations in the aviation industry were found to be more likely to share item-level data in the study. Companies would share product's lifecycle data with other partners. In the pharmaceutical industry relevant product information data would be shared in case that a pedigree is required. Information would be made accessible downstream. Overall, the study suggests that data sharing should be limited to a specific set of applications and data should only be used for a predefined purpose [8, 21].

Trust has been found to be a relevant factor to predict data sharing behavior in supply chains, albeit previous studies have not dealt with trust issues related to the sharing of item-level data [22–25]. Trust is a decisive and important element of business relationships in supply chains [14, 22]. According to a study of the BRIDGE project, trust is crucial in parties that use a track and trace system to authenticate products [8]. Kumar states that information can only be shared in settings, in which all involved parties trust each other [23]. Chopra and Meindl claim that managers are more likely to share information if organizations in the supply chain trust each other [17]. Yang and Jarvenpaa deem trust vital to foster cooperative behavior [25]. Trust can also help reducing costs, e.g. by reducing or even avoiding the same tests at incoming and outgoing goods inspection [23]. Moreover, a trustful business relationship tends to save transaction costs between two stages of a supply chain [17]. Therefore trust may also have an indirect impact on an organization's willingness to share data, namely via its cost-benefit-ratio. The relevance of trust has been discussed in the context of the game theory [26] and psychological investigations on so-called social dilemmas [24, 27, 28]. In addition to trust, dependencies to other organizations and power have been found to affect organizations willingness to share data [29]. Power is understood as the enacted trading partner power [30]. These factors were identified as decisive to determine the extent of shared data [29–32]. In supply chains, in which a powerful company forces its business partners to share data, trust has a lower effect on the willingness to share data than in supply chains with a more balanced power situation.

3 Methodology

By the means of the literature review, as described in Sect. 2, theories have been recognized that can partially explain the nature of data sharing, e.g. the "Theory of Games and Economic Behavior" [26] or the "Tragedy of the Commons" [28]. The literature review provides an overview of recent and relevant work, and it presents insights into business rationales, motivations and barriers to engage in data sharing in supply chains. The last paragraph of Sect. 2 is dedicated to the relevance of trust, which was found to be a decisive factor in regard to data sharing. The literature review, however, revealed that little work has been done so far to identify and assess risks that are associated with data sharing. There is hardly any literature that assesses data sharing on an item level and most literature is on a more general level. The latest advances of the Internet of Things, data sharing on item-level, and the consequent perceived privacy risks have not sufficiently been taken into account so far, causing a gap in the existing literature. As distinguished from the related work (Sect. 2; except for the work undertaken in the context of the BRIDGE project perhaps), we put a particular emphasis on those two points in our qualitative research. The research process is based on Bryman and Teevan [33]: To collect data, in-depth phone interviews that were guided by a semi-structured questionnaire with 16 experts from the industry were conducted. The willingness to share item-level event data was assessed by open questions about companies' current sharing behavior, their overall willingness to share, with whom they share, which data they share, and under which circumstances they share event data. Potential privacy risk scenarios were derived from literature and the experts were asked to assess these threats and their impact on data sharing. In order to identify further risks not mentioned in literature so far, the interviewees were asked for their expertise. One interviewee could only be interviewed about potential privacy risks and not about the level of actual sharing behavior and willingness to share. Furthermore, the interviewees were asked to describe the supply chain they are part of, including its size, complexity, level of trust, knowledge about other participants, and power balance.

In total, 16 interviews with organizations from Belgium, Germany, Switzerland and the USA took place. The experts targeted are key personnel in charge of logistics or data sharing in the supply chain. Four different industries were covered: automotive (6 participants), consumer goods (4 participants), electronics, machinery and factory construction (3 participants), and the pharmaceutical industry (3 participants). By targeting diverse industries that operate under different conditions, it was intended to gain a broad understanding of perceived risks and to explore whether data sharing obstacles are comparable or largely diverse across industries. These industries were also targeted because there is an indication that tracking and tracking based applications could be adopted by them in the future. The automotive industry is affected by counterfeiting [8] and characterized by long and diverse supply chains. The same applies to the supply chains in the electronics, machinery and factory construction industry. Furthermore, many machines can be considered expensive enough to justify the costs for an identification technology and the necessary tracking infrastructure. The consumer goods industry was selected due to its cutting edge use of RFID research and applications [9]. The pharmaceutical industry was included mainly because of electronic pedigree acts in some countries [6].

4 Willingness to share data and sharing risks

In this section, the major results of the data analysis are presented: (Sect. 4.1) description of the current sharing situation and organizations' willingness to share item-level event data, (Sect. 4.2) perceived risks with regard to privacy.

4.1 Willingness to share item-level event data

This subsection is organized as follows: in Sect. 4.1.1 the *actual* sharing of event data at item-level is presented, while Sect. 4.1.2 refers to the *willingness* to share item-level event data. It concludes with a short summary and an interpretation of the data (Sect. 4.1.3).

4.1.1 Actual sharing of event data at item-level

The extent of the current sharing behavior of an organization was assessed by regarding the following aspects: whether companies share item level data at all, the number of business partners with which data is shared, and the type of data that are shared. Organizations showing similar sharing behaviors were grouped together (Table 1).

Only 4 respondents (27%) stated that their organization currently shared item level data. In one case, item level data will have to be shared soon as a more powerful business partner urged data sharing. The organizations that shared only some data limited the sharing to selected data types, selected items or selected partners within the supply chain. The organizations that shared data to some extent typically reported of having a close and trustful relationship with their suppliers and sub-suppliers. They are part of smaller supply chains, in which most of the other organizations are known. The group of companies that shared no item-level data at all includes all interviewed companies from the pharmaceutical industry as well as all companies in the sample of companies with many suppliers and customers and which are part of large supply chains.

4.1.2 Willingness to share event data at item-level

The willingness to share data must be distinguished from the actual sharing behavior as the need for or the benefits of tracking based applications may only be revealed in

Table 1 Levels of the present actual sharing of event data at item-level

Level	Description	Total number	Percentage
0	Currently no event data at item-level is shared	11	73%
1	Currently some event data shared, but only with restrictions (only with selected business partners or only selected type of event data)	3	20%
2	Currently event data at item-level is shared, or the organization will definitely share item-level event data shortly	1	7%

Table 2 Levels of willingness of the interviewed organizations to share item-level event data

Level	Description	Number	Percentage
0	No willingness to share event data:	0	0%
	Currently no willingness to share		
1	Low willingness to share event data:	10	67%
	The willingness is low, though there is no fundamental reluctance. The sharing would be restricted to a few type of data, products, or business partners		
2	Medium willingness to share event data:	2	13%
	There is a willingness to share for some selected kind of data, products and business partners. Only under some particular circumstances the restrictions would be revoked		
3	High willingness to share event data:	2	13%
	There is a high willingness to share with a few specific exceptions		
4	Unrestricted willingness to share event data:	1	7%
	The willingness to share exists without any restriction		

the future. The willingness of companies to share event data, according to the judgment of the respondents, can be described on a five level scale from no willingness to unrestricted willingness to share event data (Table 2).

Interestingly, in no case the sharing of item level data was ruled out completely. All companies could think of some conditions under which they would share at least some data with some business partners. While 80% stated they would not share data but for a few exceptions, 13% of the companies chose the reverse approach and claimed to generally allow sharing with a few restrictions as to what or with whom not to share. The largest share (67%) of companies reported a low willingness to share, meaning that the conditions under which data is shared are imagined to be very restrictive.

General restrictions of data sharing When it comes to restrictions regarding organizations with which data is shared, respondents mentioned limiting sharing to downstream partners, while no data with upstream data should be shared at all. Some organizations can imagine sharing information with all participants of the supply chain, both up- and downstream. Indirect business partners and competitors were mentioned as to be excluded from the organizations that data would be shared with.

Regarding the kind of event data to be shared, some organizations are only willing to share data concerning deliveries and item transitions and only with business partners directly involved in the transaction. Some respondents also expressed the wish to exclude all data related to production and production processes.

The willingness to share data was higher in those companies that know their suppliers and the suppliers of their suppliers. The willingness to share event data was also higher for those companies that felt that their goals were well aligned with the goals of the other supply chain participants. The companies reporting a low willingness to share were part of large and complex supply chains with many participants.

Willingness to share event data at item-level per industry While the willingness to share item-level event data was quite low in the automotive and consumer goods industry, it was reported to be even less in the pharmaceutical industry and in the electronics, machinery and factory construction industry.

In the *automotive industry* the power balance was identified to be decisive to determine the extent of shared data, besides the perceived risks and trust. The more power an organization has with respect to its business partners, the lower the willingness to share will be, while a small amount of power correlates with a high willingness to share data. The last holds true only in those supply chain settings where a powerful company forces its business partners to share data. The data analysis of the empirical study revealed that "weak" organizations are very likely to disclose their item-level event data to powerful companies in the same supply chain. This behavior is due to the enacted trading partner's power. The overall reluctance to share item-level found in this study is inline with the findings of the study of the BRIDGE project [8]. However, our study revealed that in spite of the overall reluctance, some "weak" organizations would comply with a request of a more powerful company in the supply chain in order to keep the business relationship. Companies in the automotive industry would appreciate an inventory inaccuracies reduction and a more efficient warehouse management. Trust in and dependency on business partners are high and could explain why companies would comply with a sharing request.

In the *consumer goods industry*, concerns about the price maintenance are prevalent. Organizations' reluctance to share in this industry mainly stem from potential negative consequences of risks including the threat to be penalized after detection of inefficiencies or for unfair behavior, the reconstruction of strategic decisions, and the difficulty in justifying the price. The results of our study are consistent with those of the study of the BRIDGE project [8] in the finding that the consumer goods industry is among those industries which are the most willing to share event data. However, our study is contradictory to the extent of the overall willingness to share. Even though organizations in the consumer goods industry are relatively more likely to disclose than organizations in other industries, they are still rather reluctant to share.

In *electronics, machinery and factory construction* the willingness to share event data is low. The results from the study suggest that the main reason for the low willingness is that the interviewees could not see any convincing benefits for their companies. The perception of potential risks that go along with shared event data is surprisingly low.

In the *pharmaceutical industry* a possible reconstruction of strategic decisions, relying on wrong data, and a revelation of distribution channels were perceived as the most terrific risks. Moreover, the level of trust in the supply chain partners was rather low. On the contrary to the interviews of the BRIDGE project [8], the interviews of our empirical study revealed a very low willingness to share event data in the pharmaceutical industry. The low willingness that we found in our study may be related to the fact that we conducted the interviews in states without electronic pedigree acts. Even if an automated counterfeit detection is highly appreciated in the pharmaceutical industry, risks outweigh this benefit.

4.1.3 Summary and interpretation

These findings suggest that the current level of item-level data sharing is low. This might also be attributable to a lack of tracking infrastructures and applications that make sense of the data. The general willingness of companies to share data in the future (given appropriate infrastructures and applications) can be described as low. Companies wish to restrict the event data to be shared and control with whom it is shared and which type of data are disclosed. The results of the study suggests that companies worry more about which organizations might get their data than about which types of data is shared. However, this supposition could also be explained by the unfamiliarity of the respondents with the event data model.

Concerning the actual sharing behavior as well as the overall willingness to share data, the size and complexity of the supply chain are supposed to be factors that correlate with the extent of sharing. In small supply chains, in which most or even all participants are known, the willingness to share was found to be higher than in large and complex supply chains. This coherence could be attributed to a higher level of trust in business partners in small supply chains or to an easier way of controlling the use or misuse of data combined with a higher possibility to identify and penalize harmful behavior.

4.2 Risks associated with item-level data sharing

The suspected negative consequences of or perceived risks associated with data sharing is one factor that affects the willingness to share item-level data. It can thus be drawn on to explain the low reported willingness to share. Perceived risks can reduce a company's willingness to share data and make them restrict the extent of event data to be shared even more (e.g. in terms of type, temporal availability, and number of recipients). Although there are few reports of risks associated with sharing data on item-level, a number of risks that have been described in the general context of inter-organizational data sharing can be assumed to apply also for item-level sharing. Potential risks that have been derived from literature are described, followed by a description of how relevant and threatening the risks were perceived by the study participants (Sect. 4.2.1). Furthermore, a set of additional risks revealed in the interviews which could be relevant for item-level data sharing are presented in Sect. 4.2.2.

4.2.1 Identified risks

Description of identified risks On the basis of a literature review we identified the following risks:

1. *Reconstruction of strategic decisions*: The connection of event data from different locations enables the disclosure and reconstruction of strategic decisions. Sharing of fine-granular event data increases the visibility of operations for all companies involved. If confidentiality is not preserved, a competitor could anticipate a company's future plans, e.g. an extension of the product range. An extension of the product range can be estimated if new strategic relationships are built in the supply chain and by looking at the types of items delivered. An upcoming sales

campaign of a competitor might be predicted by analyzing demand figures [34]. A higher demand from supply chain partners or the intensification of a strategic relationship might be a hint for a sales campaign or an entry to a new market.

2. *Relying on wrong data*: Access to supply chain-wide information may be beneficial to the individual companies, but there is a concern whether the business partners will sincerely share their information. It is assumed that the market of EPC traces will be vulnerable to moral hazard, to actors who sell "fake traces" [35]. Competitive partners may intentionally manipulate the data they share or even inject completely false data [36]. Incomplete data limits the reliability of data analyses. False data, however, like "false traces", might even negatively affect the analyses. Inaccurate analyses may result in wrong business decisions and may have economic repercussions.
3. *Threat to be penalized for unfair behavior*: Increased visibility not only allows for the detection of inefficient behavior, but also of unfair behavior, i.e. the "little tricks" that companies apply to gain a better competitive position. For example, in case of a supply bottleneck, it is assumed that some buyers have an incentive to overstate their actual demand in order to gain a better share of the items in short supply. This behavior might not work anymore if event data is shared on item-level. In other words, the affected company will not get a higher share of items in short supply and might not meet its customers' demands [14]. Another example of unfair behavior is to induce the suppliers to carry high inventory at their expense by exaggerating the demand.
4. *Lose in a* "*race to learn*": In an environment where item-level event data is shared, some organizations might seek to learn with an exploitative intent, e.g. to infer best practices, or reliable sources of materials. To improve each company's competitive advantage, this attitude may lead to a so-called "race to learn" [35]. One company will win, but the other may not.
5. *Loss of information advantages*: Disclosing sales information to other organizations may reduce the effect of so-called information rents from which especially weaker parties in the supply chain currently profit. A loss of the information rent may change the relationship of the business partners [37].
6. *Revelation of distribution channels*: Increased visibility may reveal the distribution channels and the routes of individual items. With this information terrorists and potential thieves could estimate when an item is passing a weak point in the supply chain [7, 19, 21].
7. *Threat to be penalized after detection of inefficiencies*: As complete event data allows for a fine-granular view of what happened to individual items and when, this might allow companies to detect and potentially penalize inefficient behavior of their business partners, e.g. up to a change of suppliers. Consider the following example: One of the most important attributes of an event is its time stamp. By sharing time stamped events that also contain location information, it becomes possible to determine when a company's custody of a product (physical ownership of the product) starts and when it ends. The time stamps allow the calculation of how long a specific product was stored in one particular location. With this information, "sloppiness" in companies' operations can be detected and the company might get penalized for storing the product too long, e.g. in case the delivery is

Table 3 Perceived threat level of a risk

n/a	This risk does not apply to my company
1	This risk has only a small impact on my company's data sharing policy
2	This risk has quite some impact on my company's data sharing policy
3	This risk is a decisive factor that hinders my company from sharing item-level event data
4	As long as this risk exists, my company will definitely not share any item-level event data

Table 4 Relevance of risk types and perceived threat level

Risk	Percentage of affected companies	Mode	Minimum	Maximum
Reconstruct strategic decisions	93%	3	1	4
Relying on wrong data	71%	1	1	4
Threat to be penalized for unfair behavior	63%	1	1	4
Lose in a "race to learn"	50%	1, 2, 3	1	4
Loss of information advantages	50%	2	1	3
Identify distribution channels	47%	1	1	4
Threat to be penalized after the detection of inefficiencies	44%	1	1	4

time-critical. An example of this scenario is a company storing too many items within its store at the expense of another company [38]. The traceability and the visibility of items would provide the means for other companies to detect capacity problems and use them to renegotiate conditions.

In order to explore whether these risks are considered as relevant by companies and to what extent a risk affects a companies willingness to share item-level data, the study participants were asked to indicate the potential impact of the risk on the data sharing policy on a 5 point scale (Table 3).

Assessment of identified risks In order to analyze the impact of these seven risks we asked the interviewees about each identified risk if it applies to their company and what impact each risk has on their company's data sharing policy. The interviewees could rate the impact and the risk level of each risk according to a predefined code (Table 3). The median, mode, minimum, and maximum was calculated based on this code (Table 4).

The risk perceived by most companies as relevant is the reconstruction of strategic decisions (reported by 93%). A high relevance was also attributed to the risk of relying on wrong data injected by competitors (71%). Being penalized for unfair behavior is the third most frequent mentioned risk (63%), and perceived as more relevant than being penalized for inefficiencies (44%). Each risk was perceived to be relevant by at least 44% of the respondents, meaning that none of the assumed risks is negligible.

Besides being the risk perceived as most relevant, the risk that competitors might reconstruct strategic relationships was also the risk with largest influence on the sharing behavior of companies. Most companies perceived this risk as so threatening that

it would severely limit their sharing behavior. The loss of information advantages was also perceived as quite threatening by many companies. Most companies that mentioned that risk as relevant assessed it as having some impact on the data sharing policy, but not restricting data sharing as much as the reconstruction of strategic decisions. The expected impact of a loss in a race to learn on the extent of data sharing varies across respondents, while for all other risks the majority of respondents found them to have only a minor impact on the sharing policy. For all risks (except for "loss of information advantages"), the full spectrum of possible impacts on the data sharing policy—from minor impacts to a complete halt of data sharing—could be observed. Further analysis revealed that 25% of the organizations will definitely not share any item-level event data at all, as long as a particular risk exists. 75% of the organizations in the sample rate at least one risk as a decisive factor hindering the company from sharing data or even prevents inter-organizational sharing completely.

4.2.2 Newly revealed risks

Besides the risks that were known to exist from literature, study participants also mentioned a number of further risks that are specific to the sharing of item-level data:

1. *Development of a competitive product*: A competitive product might be developed with the knowledge of suppliers and sub-suppliers. Competitors might get in touch with top suppliers.
2. *Weakening of the bargaining power after disclosure of purchase or supply volume*: A customer could compare its own purchase volume to the purchase volumes of other customers and calculate its share. This information might be used by strategic buyers to strengthen their bargaining power. Respectively, suppliers could calculate their share of overall supply. This information contributes to determine the power of a supplier and the dependence of a recipient on a supplier.
3. *Difficulty in justifying the price*: The sharing of event data could reveal the source of single items and semi-finished components. The customer could make inquiries into delivered quantities and prices. The inquiries might enable her/him to claim a lower price.
4. *Concerns about the price maintenance*: The disclosure of distribution channels could enable customers to descry similar products. Costumers may perceive similar products as being equivalent, even though the products are not of the same quality. For instance, similar products could be made up of the same components but differ in quality due to different manufacturing techniques. The customer might not appreciate the more sophisticated manufacturing technique and therefore choose the cheaper product or claim a lower price for the more sophisticated product.
5. *Skipping a stage in the supply chain*: Intermediate stages in the supply chain might be skipped if the organizations are acting primarily as intermediaries. For example, manufacturers might contact customers directly after inferring the buyers contact details from the data. They might also directly offer repair or maintenance services. Particularly small-sized businesses are concerned that they could easily be substituted or become obsolete.

6. *Loss of know how*: Expertise might become accessible to competitors if production sequences could be reconstructed (cf. aggregation event [5]) revealing which components are assembled in which products and in which sequence. Competitors could use this information to improve their production or to imitate a product.
7. *Increased mistrust*: The electronic processing of data can contribute to an automatic managing of procedures and to a reduction of the necessity of personal communication. Some respondents were worried about increasing mistrust and a decrease of partnership.

4.2.3 Summary and interpretation

The results of this study suggest that most of the newly found risks—and actually even most risks overall—have their source in parallel streams of the supply chain, in which companies compete with each other. Companies of the same stage but of different streams may be competitors that are afraid of revealing any data. Another thread is the mistrust in other supply chain partners that is expressed by the overall agreement that business partners or even unknown actors in the supply chain might use the data to the disadvantage of companies that share.

5 Implications

The reluctance of organizations to share event data at item-level imposes difficult challenges to the security area. Appropriate measures that mitigate the risks must be designed in order to gain more trust in sharing data, which is a prerequisite to achieve the benefits of tracking applications. Designers of privacy and security mechanisms are challenged to develop concepts that allow limiting the visibility of event data in a way that specific benefits can be reaped and risks mitigated. A critical success factor is to provide customized solutions, as the requirements of companies are diverse and each type of risk may require a different solution concept. The risk perceived as most severe was the reconstruction of strategic relationships. When examining this risk more closely, it is apparent that the exact data that is affected and thus the possibilities to mitigate this risk depend largely on the company and the kind of strategically important decisions a specific company takes. This scenario dependence can also be observed for most of the other risks. There is no predefined set of data (types), conditions or business partners that, when excluded from sharing, would mitigate a risk for all companies. It is thus required that any measure designed to minimize data sharing risks must be flexible and adaptable enough to cater for the requirements of different organizations.

We believe that the presented list of risks is not only useful in designing appropriate privacy and security mechanisms, but also in evaluating existing concepts for their suitability in the context of item-level data sharing between organizations. Some of the identified risks translate directly to quality criteria for security mechanisms, such as the inability to reconstruct strategic relationships, the inability to detect unfair behavior respective inefficiencies, or the inability to identify distribution channels.

Apart from using traditional security metrics, being able to demonstrate that a mechanism is able to provide these features would be suitable to make research in the security domain more relevant to a managerial audience.

After having conducted the expert interviews, meetings with system security experts from academia and industry followed. The discussions brought three basic ways to light that could help to reap the benefits of tracking applications while minimizing the aforementioned risks:

1. Devise a fine grained *access control system* that fulfills the stated requirements. For example, risks were described in Sect. 4.2 that are connected to the calculation of how long a specific product is stored in one particular location. This calculation only works precisely if the time stamps at both goods receipt and goods issue are accessible. Even if access is denied to one part of this time data, many e-commerce (meta-) services still work. For targeted product recalls, for example, the goods receipt timestamp is sufficient to know where the product is. Our colleagues Zanetti and Capkun already presented a fine-grained access control mechanism to detect and prevent the leakage of sensitive business information while sharing serial-level data [39]. Their solution is composed of a framework for describing relations between sensitive information (e.g. volumes) and serial-level data (e.g. both timestamps and the number of data), and of a security architecture that, based on predefined relations, detects and prevents the leakage of sensitive information while sharing serial-level data [39].
2. Use methods related to *secure multi-party computation* that are, to a certain degree, able to compute a result without revealing data [40, 41]. During its execution, a secure multi-party computation protocol guarantees a predefined level of security depending on the chosen attacker model (semi-honest or malicious). The protocol does not (generally) guarantee security on what can be inferred from the output of the protocol itself. Thus, any function can be considered. Crypto tools to implement functions in a privacy-preserving way exist, but they can be very impractical due to their complexity: it may take a long time to run secure multi-party protocols for even non-so-complex functions among a relatively small number of players. For instance, with the solution proposed by Ben-David et al. [42], seven participants can compute a function that can be represented as a 1024 gate circuit in almost 10 seconds. If such a computation needs to be carried out for each tag this would probably take months, maybe even years. In the context of supply chains, Atallah et al. [43, 44] proposed several privacy-preserving protocols for capacity allocation, e-auctions, and collaborative planning, forecasting, and replenishment.
3. Every participant shares data with a *trusted third party*. Only the trusted third party has access to the raw data and propagates the results necessary to achieve the benefits of inter-organizational tracking applications back to the individual participants. A critical success factor will be how to answer the question of who would be a suitable, trusted organization that could play such a role, e.g. for a certain industry. Consider, for example, a pharmaceutical supply chain, in which pharmaceutical counterfeits are circulating. As Florida and California passed laws that require pedigrees to be transmitted of all prescriptions drugs, it may seem likely that governmental institutions may take the role of the trusted third party.

This may even lead to an advantage for police and customs by being notified immediately to confiscate tampered pharmaceuticals as soon as it becomes evident. As for the secure computations, another success factor might be to avoid one party to infer critical information from the results distribute by the third party.

6 Conclusion and outlook

In the study we found that the current sharing of item-level event data as well as the willingness to share event data is low for the participating companies. Companies wish to impose many restrictions in terms of data recipients and data types, but the restrictions vary across companies. As a decisive factor contributing to the low willingness to share data, privacy risks could be identified. There is no general severity of a risk, but the perceived threat depends on the specific conditions under which a company operates. The study revealed that there are many and diverse risks associated with sharing item-level data. While many of the risks apply as well to data sharing on an aggregated level, additional risks that are specific to item-level sharing were reported. In case item-level data is shared, the number of potential risks increases as the information is finer grained and individual items instead of bulks are visible. The number of risks increases when data is not only shared, but even shared on item-level.The reconstruction of a company's strategic decisions and the loss of information advantages were identified as the risks perceived as most threatening. A flexible way of describing restrictions and a possibility to enable reasonable sharing with unknown organizations are requirements that need to be taken into account when designing inter-organizational tracking and data sharing infrastructures.

Trust has been found to be a significant factor that heavily impacts an organization's willingness to share data. The study suggest that the size of the supply chain and the fact whether most of the other supply chain participants are known, has a major influence on the willingness to share data. In large and complex supply chains with many participants, the willingness to share is generally lower than in small supply chains. Suitable measures for mitigating the identified risks need to be developed to gain more trust in sharing data. Apart from the three suggested alternatives (access control system, secure multi-party computation, trusted third part) for achieving data privacy, different approaches might be needed or perform better.

The study is limited by the small sample size that does not allow to draw general conclusions. However, we are among the first to explore this area and thus a small sample size and in-depth interviews seemed to be suitable.

For further exploring the risks associated with data sharing on item-level, a survey with a larger number of participants would be suitable. It needs to be investigated which risks are specific to certain industries or supply chain types, so that systems that fulfill the requirements of specific sets of companies can be designed. Moreover, it is required to analyze the desired restrictions more precisely and develop appropriate ways of describing them formally.

We believe that without a detailed understanding of the potential risks associated with data sharing, no suitable countermeasures can be developed. This paper thus contributes a set of privacy risks that developers of inter-organizational data sharing

systems should take into account when developing systems and against which existing systems can be tested. The set of risks might help a managerial audience to better understand what consequences data sharing might have and may be used to state specific requirements for risk mitigation.

References

1. Floerkemeier, C., Langheinrich, M., Fleisch, E., Mattern, F., & Sarma, S. E. (2008). *The internet of things: Proceedings of the 1st international conference*, Zurich, Switzerland. Berlin: Springer.
2. Schuster, E., Allen, S., & Brock, D. (2007). *Global RFID—the value of the EPCglobal network for supply chain management*. Secaucus: Springer.
3. Agrawal, R., Cheung, A., Kailing, K., & Schonauer, S. (2006). Towards traceability across sovereign, distributed RFID databases. In *Proceedings of the 10th international database engineering and applications symposium* (pp. 174–184). New Delhi: IEEE Comput. Soc.
4. EPCglobal Inc. (2007). EPC information services (EPCIS) version 1.0.1 specification. http://www.epcglobalinc.org/standards/epcis/epcis_1_0_1-standard-20070921.pdf.
5. Timmers, P. (1998). Business models for electronic markets. *Electronic Markets*, *8*(2), 3–8.
6. VeriSign Inc. (2005). Beyond pedigree: the role of infrastructure in the pharmaceutical supply chain. http://www.verisign.com/static/031078.pdf. White Paper.
7. Staake, T., Thiesse, F., & Fleisch, E. (2005). Extending the EPC network—the potential of RFID in anti-counterfeiting. In *Proceedings of the 2005 ACM symposium on applied computing* (pp. 1607–1612). New York: ACM Press.
8. ETH Zurich & SAP Research (BRIDGE) (2007). Anti-counterfeiting requirements report. http://www.bridge-project.eu/data/File/BRIDGE%20WP05%20Anti-Counterfeiting%20Requirements%20Report.pdf.
9. Curtin, J., Kauffman, R., & Riggins, F. (2007). Making the 'MOST' out of RFID technology: a research agenda for the study of the adoption, usage and impact of RFID. *Information Technology and Management*, *8*(2), 87–110.
10. Koh, R., Schuster, E., Chackrabarti, I., & Bellman, A. (2003). Securing the pharmaceutical supply chain. http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH021.pdf.
11. Ilic, A., Michahelles, F., & Fleisch, E. (2007). The dual ownership model: using organizational relationships for access control in safety supply chains. In *Proceedings of the 21st international conference on advanced information networking and applications workshops* (pp. 459–466). Washington: IEEE Comput. Soc.
12. Premkumar, G. (2000). Inter-organizational systems and supply chain management—an information processing perspective. *Information Systems Management*, *17*(3), 56–69.
13. Yu, Z., Yan, H., & Cheng, T. (2001). Benefits of information sharing with supply chain partnerships. *Industrial Management & Data Systems*, *101*(3), 114–121.
14. Lee, H., & Whang, S. (2000). Information sharing in a supply chain. *International Journal of Technology Management*, *20*(3/4), 373–387.
15. Cachon, G., & Fisher, M. (2000). Supply chain inventory management and the value of shared information. *Management Science*, *46*(8), 1032–1048.
16. Li, J., Shaw, M., Sikora, R., Tan, G., & Yang, R. (2001). The effects of information sharing strategies on supply chain performance. http://citebm.cba.uiuc.edu/B2Bresearch/ieee_em.pdf.
17. Chopra, S., & Meindl, P. (2004). *Supply chain management: strategy, planning, and operation* (2nd international edn.). Upper Saddle River: Pearson Education International/Prentice Hall, 492 et seq.
18. Bresser, R. (1988). Matching collective and competitive strategies. *Strategic Management Journal*, *9*(4), 375–385.
19. BT Research, ETH Zurich, Technical University Graz, SAP Research, AT4 wireless, Benedicta, Universitat de Catalunya, Caen, Confidex, Fudan University, UPM Rafalatac, & GS1 UK (BRIDGE) (2007). Security analysis report. http://www.bridge-project.eu/data/File/BRIDGE%20WP04%20Security%20Analysis%20Report.pdf.
20. Building Radio Frequency IDentification for the Global Environment (BRIDGE) (2009). http://www.bridge-project.eu.

21. Cambridge University, BT Research, & SAP Research (BRIDGE) (2007). Serial-level inventory tracking model. http://www.bridge-project.eu/data/File/BRIDGE%20WP03%20Serial-Level%20inventory%20tracking%20Model.pdf.
22. Child, J., Faulkner, D., & Tallman, S. (2005). *Cooperative strategy: managing alliances, networks, and joint ventures*. New York: Oxford University Press, 50 et seq.
23. Kumar, N. (1996). The power of trust in manufacturer-retailer relationships. *Harvard Business Review*, *74*(6), 92–106.
24. Axelrod, R. (1984). *The evolution of cooperation*. New York: Basic Books.
25. Yang, G., & Jarvenpaa, S. (2005). Trust and radio frequency identification (RFID) adoption within an alliance. In *Proceedings of the 38th annual Hawaii international conference on system sciences* (Track 7, Vol. 7). Washington: IEEE Comput. Soc., 208.1.
26. von Neumann, J., & Morgenstern, O. (1994). *Theory of games and economic behavior*. New York: Wiley.
27. Olson, M. (1965). *The logic of collective action*. Cambridge: Harvard University Press.
28. Hardin, G. (1968). The tragedy of the commons. *Science*, *162*, 1243–1248.
29. Hart, P., & Saunders, C. (1997). Power and trust: critical factors in the adoption and use of electronic data interchange. *Organization Science*, *8*(1), 23–42.
30. Chwelos, P., Benbasat, I., & Dexter, A. (2001). Empirical test of an EDI adoption model. *Information Systems Research*, *12*(3), 304–321.
31. Iacovou, C., Benbasat, I., & Dexter, A. (1995). Electronic data interchange and small organizations: adoption and impact of technology. *MIS Quarterly*, *19*(4), 465–485.
32. Reekers, N., & Smithson, S. (1995). The impact of electronic data interchange on interorganizational relationships: integrating theoretical perspectives. In *Proceedings of the 28th Hawaii international conference on system sciences* (Vol. 4, pp. 757–766). Washington: IEEE Comput. Soc.
33. Bryman, A., Teevan, J., & Teevan, J. (2005). *Social research methods* (Canadian edn.) (p. 146). Don Mills: Oxford University Press.
34. Du, W., & Atallah, M. (2001). Privacy-preserving cooperative statistical analysis. In *Proceedings of the 17th annual computer security applications conference* (p. 102). Washington: IEEE Comput. Soc.
35. Bauer, M., Fabian, B. M., Fischmann, M., & Gürses, S. (2006). Emerging markets for RFID traces. http://arxiv.org/PS_cache/cs/pdf/0606/0606018v1.pdf.
36. Zhang, N., & Zhao, W. (2005). Distributed privacy preserving information sharing. In *Proceedings of the 31st international conference on very large data bases* (pp. 889–900). Trondheim: VLDB Endowment.
37. Li, L. (2002). Information sharing in a supply chain with horizontal competition. *Management Science*, *48*(9), 1196–1212.
38. Evans, N. (2004). Planning for RFID data. *RFID-Journal*. http://www.rfidjournal.com/article/articleview/1004/1/82/.
39. Zanetti, D., & Capkun, S. (2008). Protecting sensitive business information while sharing serial-level data. In *Proceedings of the 2008 12th enterprise distributed object computing conference workshops* (pp. 183–191). Washington: IEEE Comput. Soc.
40. Agrawal, R., Evfimievski, A., & Srikant, R. (2003). Information sharing across private databases. In *Proceedings of the 2003 ACM SIGMOD international conference on management of data* (pp. 86–97). New York: ACM.
41. Agrawal, R., & Srikant, R. (2000). Privacy-preserving data mining. In *Proceedings of the 2000 ACM SIGMOD conference on management of data* (pp. 439–450). New York: ACM.
42. Ben-David, A., Nisan, N., & Pinkas, B. (2008). FairplayMP: a system for secure multi-party computation. In *Proceedings of the 15th ACM conference on computer and communications security* (pp. 257–266). New York: ACM.
43. Atallah, M., Elmongui, H., Deshpande, V., & Schwarz, L. (2003). Secure supply-chain protocols. In *Proceedings of the IEEE international conference on e-commerce* (pp. 293–302).
44. Atallah, M., Blanton, M., Deshpande, V., Frikken, K., Li, J., & Schwarz, L. (2005). Secure collaborative planning, forecasting, and replenishment. Working Paper, Purdue University.

Markus Eurich works as a scientific collaborator at the Swiss Federal Institute of Technology Zurich with a research focus on business models for information and communication technology (ICT) innovations. He belongs to the research group of Prof. Dr. Roman Boutellier at the Department of Management, Technology, and Economics (D-MTEC). He also works in the Smart Items Research Program at SAP Research

in Zurich. He joined SAP in 2001 and mainly worked in research and in the fields of internal business consulting and customer relationship management in Germany and India. He is involved in the European research project SENSEI (Integrating the Physical with the Digital World of the Network of the Future), in which he is leading in the area of business modeling and value creation.

Nina Oertel is a research associate at the SAP Research CEC Karlsruhe. She is working in the area of Smart Items, particularly on RFID, organic electronics and tracking systems. Her research interests include the design and benefits of business applications that utilize ubiquitous technologies.

Roman Boutellier is since 1st October 2008 Vice President Human Resources and Infrastructure of ETH Zurich. He is professor and leads the Chair for Technology and Innovation Management at the Department of Management, Technology, and Economics (D-MTEC) at ETH Zurich since 2004. Since 1999 Prof. Dr. Boutellier is titular professor at the University of St. Gallen (HSG). In 1979 he received his Ph.D. in mathematics and worked as postdoctoral fellow at the Imperial College in London. His works appeared in R&D Management, Harvard Business Manager, ZFO and Drug Discovery Today. Roman Boutellier has held several leading positions in the industry and he is member of the board of directors of several Swiss large-scale enterprises. The focus of his research is the management of technology driven enterprises with a specific focus on innovation.